RSAC 2025 Conference

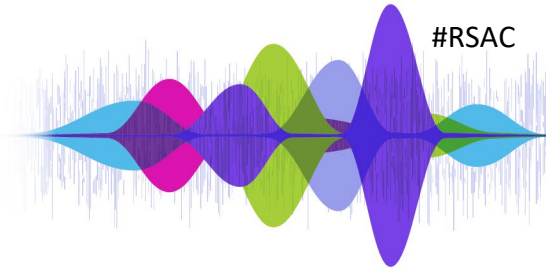
Many Voices.
One Community.

SESSION ID: PART1-W08

Asset Inventory: Your Security Blind Spot

David Dalling
GVP Global Cyber Strategist
Splunk
www.linkedin.com/in/daviddallingjr/

John Taylor
Deputy CISO
Johns Hopkins University and Medicine
www.linkedin.com/in/john-taylor-38b8754/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

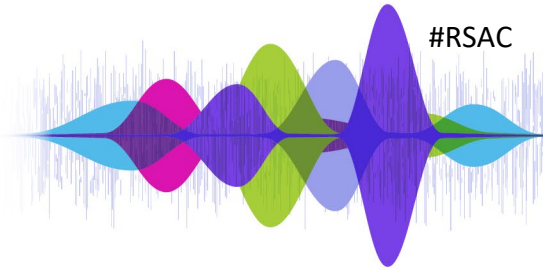
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.

Session Overview



1. What makes asset management challenging today?
2. How has Johns Hopkins University and Medicine tackled these challenges?
3. How can you evolve asset management to elevate your overall security program?

RSAC™ 2025 Conference

What makes asset management challenging today?

Many Voices.
One Community.

The SecOPs Struggle

Incomplete and

Inaccurate Asset Data

The SecOPs Struggle

Incomplete and

Inaccurate Asset Data

Lengthy Security Investigations

The SecOPs Struggle

Incomplete and

Inaccurate Asset Data

Lengthy Security Investigations

Gaps in Compliance

Traditional asset management tools are falling short.

Fragmented visibility

0010
01010
0101

Incomplete, inaccurate, and outdated data

Disconnected tools and data sources

69%

of organizations have experienced an attack targeting unknown or unmanaged assets

Stat: Security Hygiene and Posture Management Survey by ESG

Self-built tools and solutions offer their own challenges.

Higher initial setup, update, and maintenance times

Scalability and connectivity issues with other tools in your stack

Increased internal resource and time consumption

Liability issues and lack of qualified team expertise

$4 million

Average revenue loss due to compliance audit failures

Stat: Whitepaper: The True Cost of Compliance, Ponemon Institute

What is needed.

Comprehensive asset visibility to reduce risk exposure

Continuous updates to asset inventory to ensure it's never stale

An accurate, single source to find truth

43%

of organizations spend 80+ hours on asset discovery

Stat: Security Hygiene and Posture Management Survey by ESG

RSAC 2025 Conference

How has Johns Hopkins University and Medicine tackled these challenges?

Johns Hopkins University and Medicine

- About Johns Hopkins University and Medicine
  - Leading Academic Medical Center
    - Baltimore-Washington DC and St. Petersburg, FL
  - Johns Hopkins IT
    - 25 Separate IT groups
    - 35 cybersecurity professionals
  - Key Initiatives
    - Common Shared Windows Client and Server Images
    - Application Risk Assessments
    - Every IT Asset is managed
  - Investment in key technologies

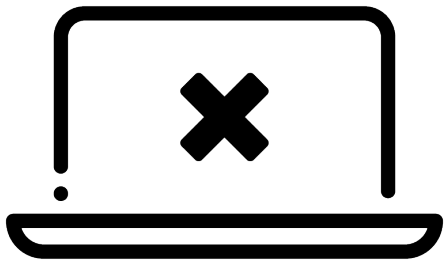
Challenges

Unmanaged systems

Unique and difficult to classify

Challenges

Unmanaged systems



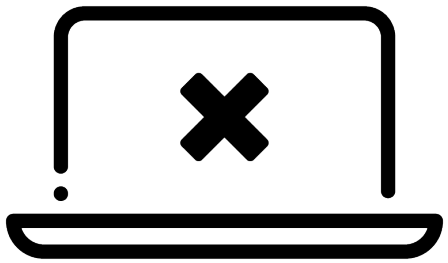
Unique and difficult to classify

Lack of insights

Existing tools not fulfilling needs

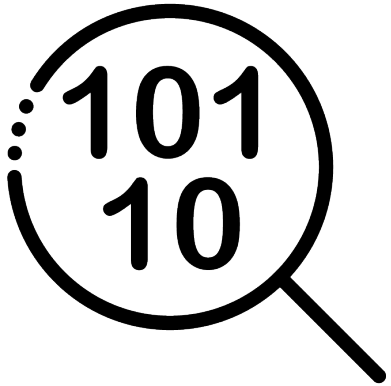
Challenges

Unmanaged systems



Unique and difficult to classify

Lack of insights



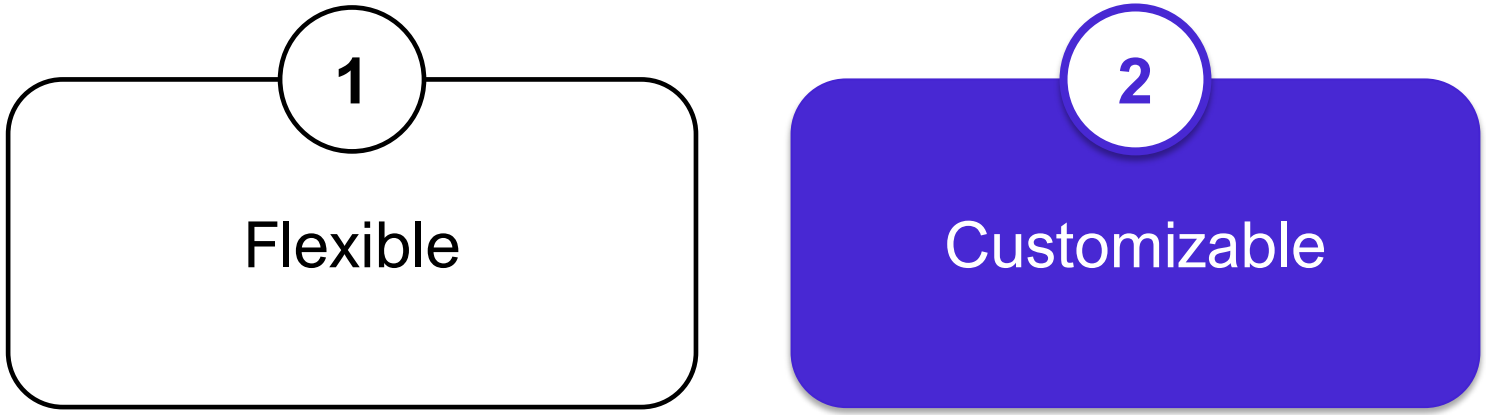
Existing tools not fulfilling needs

Maxed out capabilities

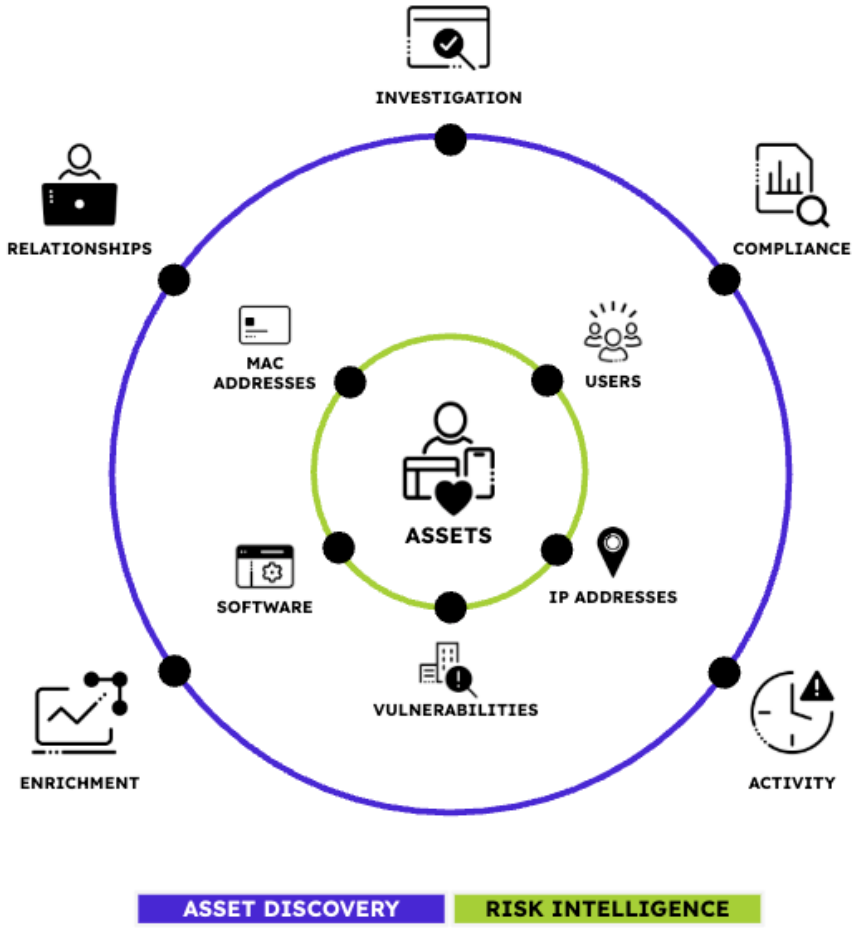
Limited options to extend tools

Problem Solving: Requirements

Problem Solving: Requirements



Problem Solving: Solution

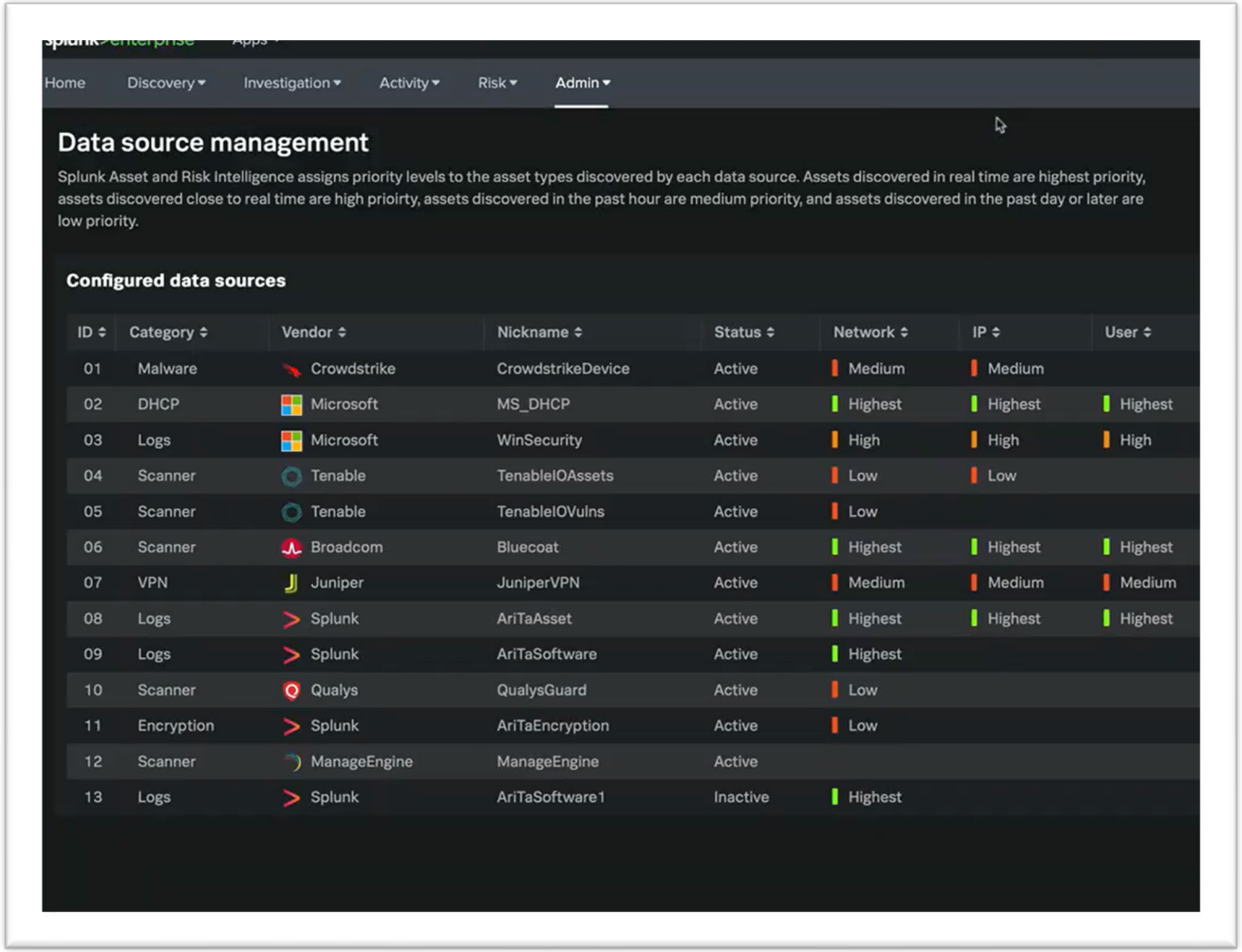


Flexible

Customizable

Problem Solving: Results

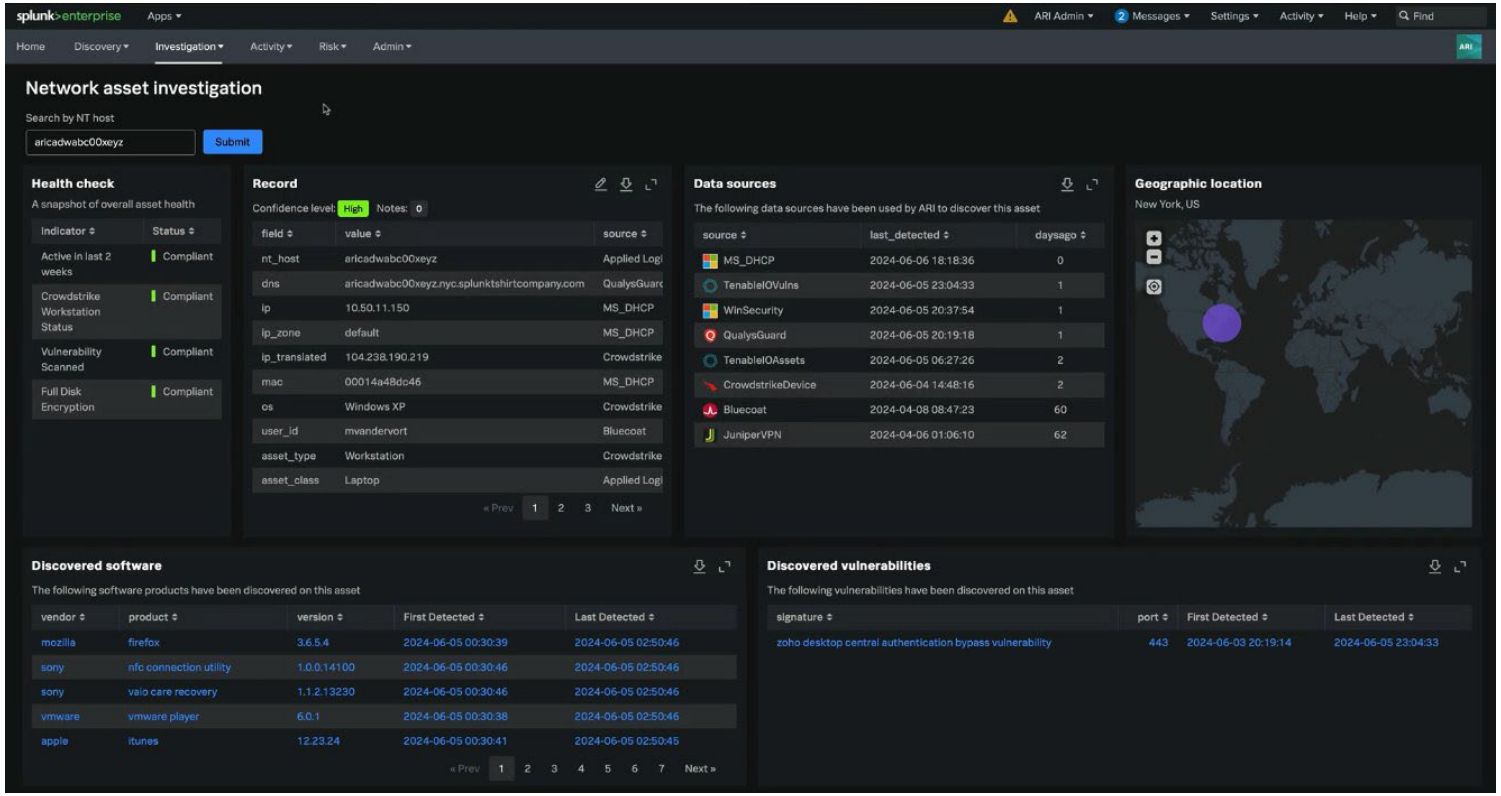
All devices identified


Home
Discovery
Investigation
Activity
Risk
Admin
Data source management
Splunk Asset and Risk Intelligence assigns priority levels to the asset types discovered by each data source. Assets discovered in real time are highest priority, assets discovered close to real time are high prioirty, assets discovered in the past hour are medium priority, and assets discovered in the past day or later are low priority.
Configured data sources

ID	Category	Vendor	Nickname	Status	Network	IP	User
01	Malware	Crowdstrike	CrowdstrikeDevice	Active	Medium	Medium	
02	DHCP	Microsoft	MS_DHCP	Active	Highest	Highest	Highest
03	Logs	Microsoft	WinSecurity	Active	High	High	High
04	Scanner	Tenable	TenableIOAssets	Active	Low	Low	
05	Scanner	Tenable	TenableIOVulns	Active	Low		
06	Scanner	Broadcom	Bluecoat	Active	Highest	Highest	Highest
07	VPN	Juniper	JuniperVPN	Active	Medium	Medium	Medium
08	Logs	Splunk	AriTaAsset	Active	Highest	Highest	Highest
09	Logs	Splunk	AriTaSoftware	Active	Highest		
10	Scanner	Qualys	QualysGuard	Active	Low		
11	Encryption	Splunk	AriTaEncryption	Active	Low		
12	Scanner	ManageEngine	ManageEngine	Active			
13	Logs	Splunk	AriTaSoftware1	Inactive	Highest		

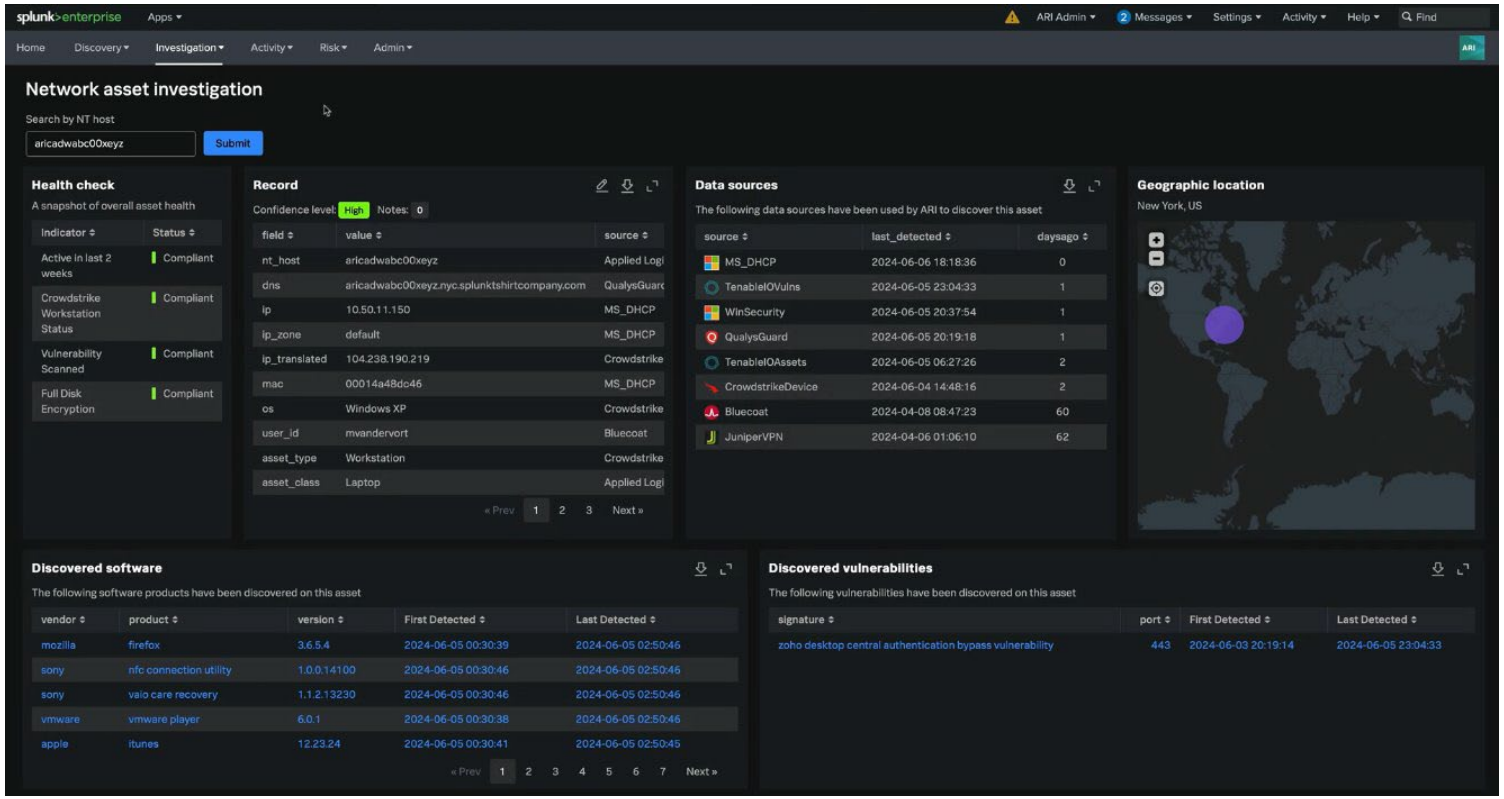
Problem Solving: Results

Devices on wrong segments isolated

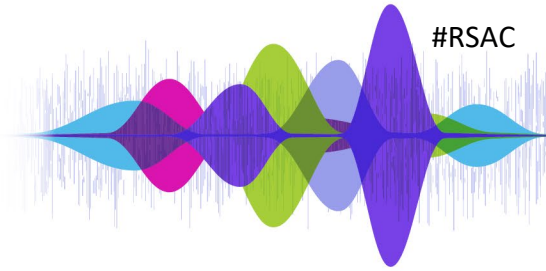


Problem Solving: Results

Devices moved to proper segments



What's Next?



1. Assessing the impact of an outage
2. Stakeholder notification system
3. MAC randomization challenges

RSAC 2025 Conference

How does an evolved asset management tool elevate your overall security program?

Empowering SecOps with Asset context

- Gain comprehensive **asset visibility** to reduce risk exposure
- Accelerate **security investigation** with accurate asset context
- Identify **compliance gaps** in security controls
- Seamless **integration** and deployment with your SIEM
- Bridge the IT and Security gap with seamless integration to your **CMDB**

Gain Comprehensive Asset Visibility

Complete and accurate asset and identity insights to reduce risk exposure.

Comprehensive asset inventory

Automatically discover and build accurate inventories of assets (including endpoints, servers, users, cloud, OT/IoT and more) leveraging data sources in Splunk.

Attribution of assets to security events

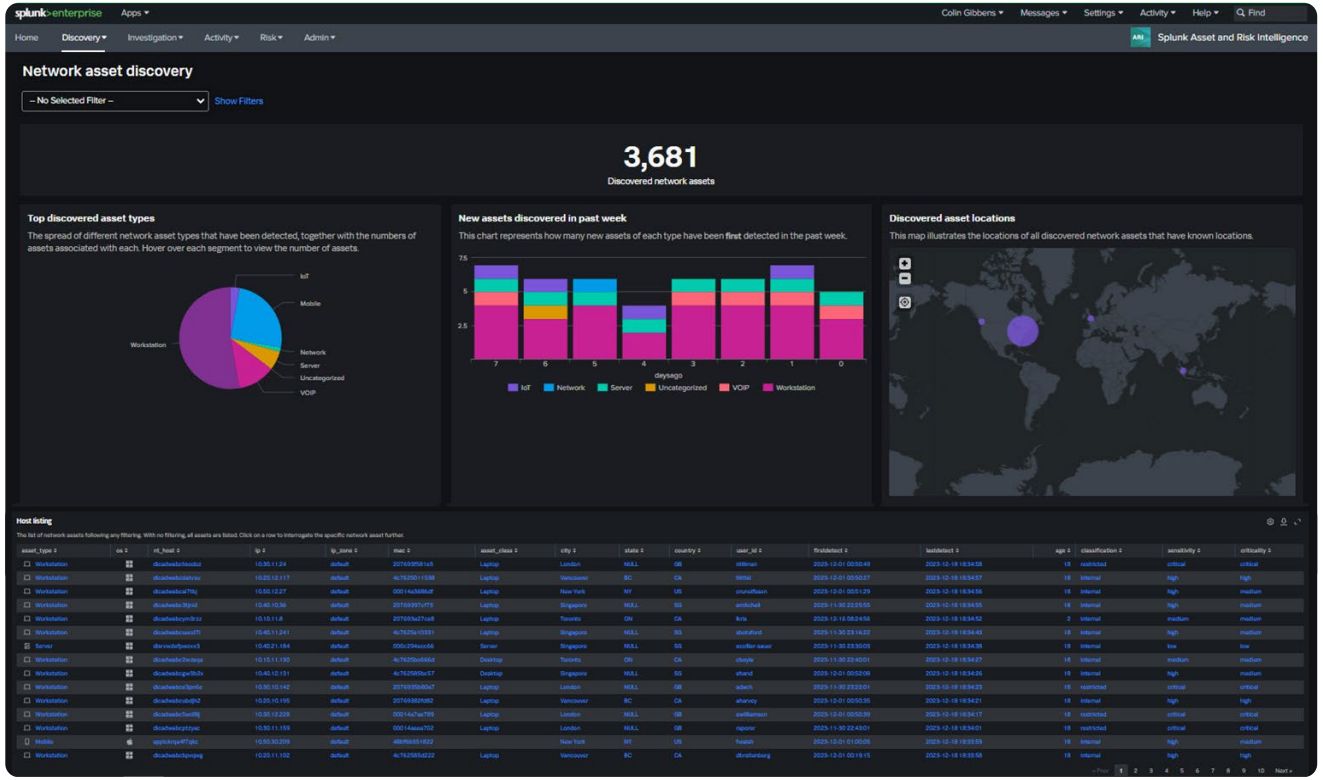
Correlate data from multiple sources into a single view per asset type (Hostname, Username, IP and MAC addresses).

Enrich and add asset context

Pull data from vulnerability and software scanning tools to inform software and vulnerabilities exist on your systems.

One asset view

Analyze asset information from multiple sources, find pattern similarities, and identify systems reporting the same asset.



Accelerate Security Investigation

Comprehensive asset and identity context to streamline investigations.

Perform instant asset investigations

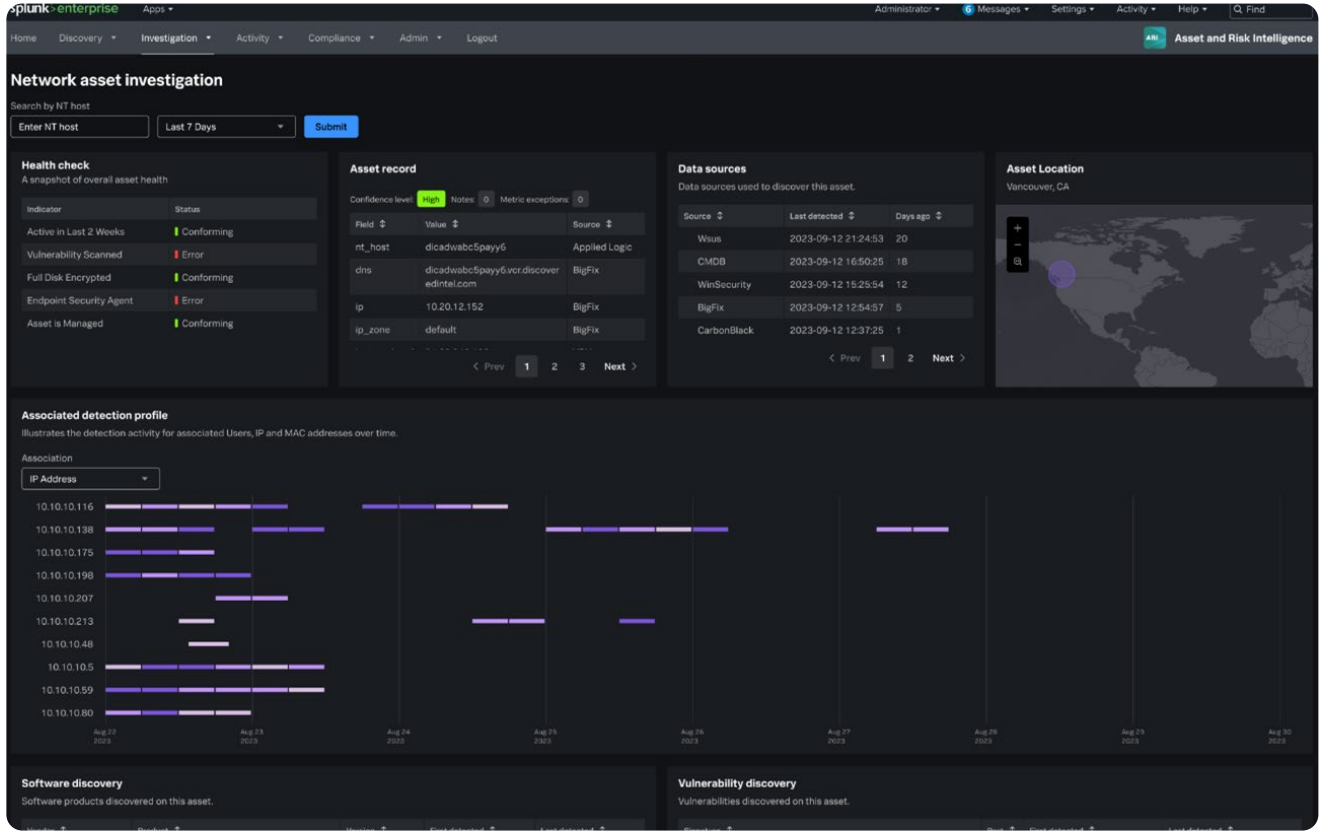
Maps relationship between assets and identities to quickly identify **who** uses **what** asset and **when** resulting in faster and more thorough investigations.

Gain holistic asset and identity insights

Instantly enrich investigations with accurate asset and identity context including network activity, asset associations, and asset health to better understand asset risk.

Streamline investigative process

Reduce time pivoting to other systems to understand the assets involved in an attack.



Discover Compliance Gaps

Combine asset discovery with continuous endpoint compliance to close gaps.

Compliance overview

Identify gaps in security controls and where you are at risk of failing an audit.

Validate compliance status

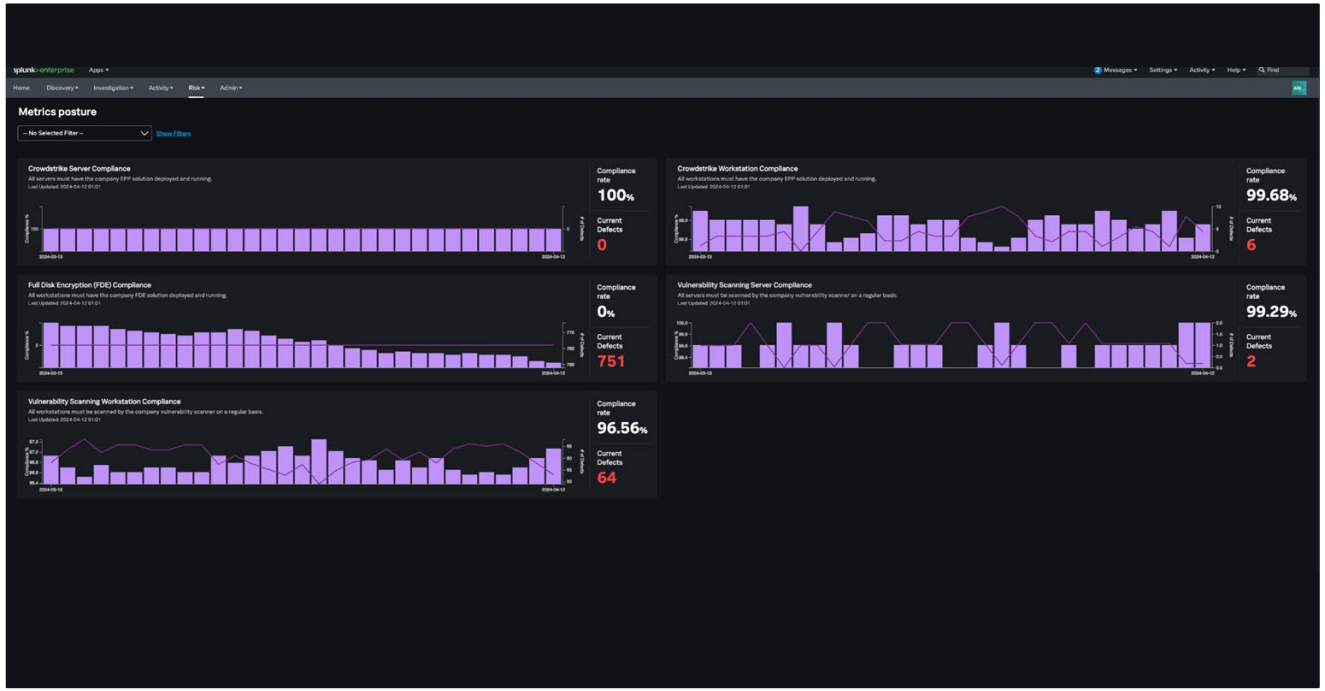
Quickly understand your compliance posture with OTTB dashboards and metrics.

Custom compliance frameworks

Build custom compliance metrics (laptop encryption, vulnerability scanning coverage, application enforcement, malware protection, and more) and report on real-time compliance against security controls.

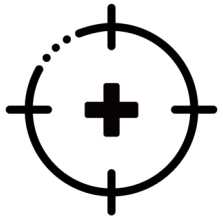
Demonstrate compliance improvements

Proactively identify compliance gaps as they occur and demonstrate improvements over time.

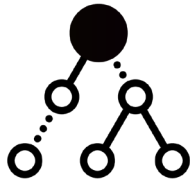


Bridging the Gap: Enhancing Asset Visibility Across IT and SecOps.

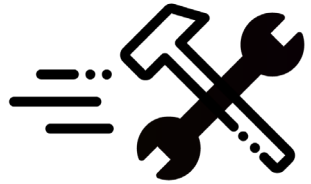
Update CMDB asset records with assets actively discovered by Asset and Risk Intelligence.



Identify unmanaged and unknown assets by populating assets discovered by Asset and Risk Intelligence that are not in ServiceNow CMDB.



Ensure CMDB data is not stale by sending unmanaged assets to ServiceNow so they are managed and update existing assets with accurate data.



Automated endpoint compliance ticketing integration send non-compliant assets to ServiceNow to generate tickets and close gaps in security.

Apply What You Have Learned Today

- Next week you should:
  - Consult the experts in your organization to start identifying the data sources that provide asset information in your environment
- In the first three months following this presentation you should:
  - Identify gaps in visibility for asset information
- Within six months you should:
  - Select a system management solution to consolidate the data from other enterprise systems

RSAC 2025 Conference

Closing Thoughts

RSAC™ 2025 Conference

Many Voices.
One Community.

For more information:
Visit Booth N-5445